JURNAL TEKNIK MESIN, ELEKTRO DAN ILMU KOMPUTER

Halaman Jurnal: https://journal.amikveteran.ac.id/index.php/teknik
Halaman UTAMA Jurnal : https://journal.amikveteran.ac.id/index.php

PERBANDINGAN PASSWORD ATTACKER MENGGUNAKAN TOOLS BARSWF, HASHCAT, HASH CRACKER CONSOLE

Decky Pratama Putra [a], I Wayan Ari Pramana Putra[b], I Gede Wahyu Parama Sucipta[c], I Made Edy Listartha[d], dan Gede Arna Jude Saskara[e]

[a] Teknik dan Kejuruan / Teknik Informatika, decky@undiksha.ac.id , Universitas Pendidikan Ganesha
[b] Teknik dan Kejuruan / Teknik Informatika, ari.pramana@undiksha.ac.id , Universitas Pendidikan Ganesha
[c] Teknik dan Kejuruan / Teknik Informatika, wahyu.pramana@undiksha.ac.id , Universitas Pendidikan Ganesha
[d] Teknik dan Kejuruan / Teknik Informatika, listartha@undiksha.ac.id , Universitas Pendidikan Ganesha
[e] Teknik dan Kejuruan / Teknik Informatika, jude.saskara@undiksha.ac.id , Universitas Pendidikan Ganesha

ABSTRACT

Password is a system or technology designed to provide authentication services to protect sensitive information that is vulnerable to attack. To protect information from such attacks, many organizations enforce complex password generation rules that require passwords to include both numeric and special characters. In this article, various password cracking programs have been examined and evaluated in detail to find out which password cracking program is most effective for knowing the passwords of a network. These password cracking programs provide information on how to perform various password attack scenarios. This article also shows the performance advantages and disadvantages of the programs tested.

.

Keywords: *: Brute force attack, Dictionary attack, Password cracking*.

ABSTRAK

Password adalah sebuah sistem atau teknologi yang dirancang untuk menyediakan layanan otentikasi untuk melindungi informasi sensitif yang rentan terhadap serangan. Untuk menjaga informasi dari serangan semacam itu, banyak organisasi memberlakukan aturan pembuatan kata sandi yang rumit dan mengharuskan kata sandi menyertakan karakter numerik dan khusus. Dalam artikel ini, berbagai macam program *password cracking* telah diperiksa dan dievaluasi secara terperinci untuk mengetahui program *password cracking* mana yang paling efektif digunakan untuk mengetahui *password* dari suatu jaringan. Program program *password cracking* tersebut memberikan informasi tentang cara melakukan berbagai skenario serangan kata sandi. Artikel ini juga menunjukkan kelebihan dan kekurangan kinerja dari program yang diuji.

.

Kata Kunci: *Brute force attack, Dictionary attack, Password cracking*.

1. PENDAHULUAN

Dalam kemajuan teknologi serta perkembangan internet yang semakin cepat ini membuat semakin banyak data yang sangat penting yang perlu dijaga. Dengan semakin terbuka nya pengetahuan hacking dan cracking, sehingga seringkali beberapa kelompok yang tidak bertanggung jawab mencoba untuk mencuri dan mengambil informasi yang ada di internet dengan teknik hacking yang beragam serta didukung dengan banyak tools yang tersedia secara gratis. Seperti yang kita ketahui tidak semua yang termasuk ke dalam kategori hacking itu jahat, terdapat tiga jenis istilah yang dapat menggambarkan seorang hacker yaitu black hat biasanya hacker yang termasuk dalam kategori anonymous atau

Received February 27, 2023; Revised March 17, 2023; Accepted March 24, 2023

berwatak antagonis, white hat mereka yang menggunakan ilmu dan pengetahuan hacking yang bermanfaat bagi keberlangsungan teknologi, dan grey hat tidak termasuk ke dalam black atau white hat, tetapi ketika grey hat sudah bisa menerobos sistem biasanya setelah itu akan dilaporkan kepada pemilik sistem tersebut.

Password attack / password cracking adalah program yang mencoba untuk membuka sebuah password yang telah ter enkripsi dengan menggunakan algoritma tertentu dengan cara mencoba semua kemungkinan. Secara teknik password cracking ini sangat sederhana, tetapi memiliki tingkat efektivitas yang tinggi, hal itu membuat tidak ada suatu sistem yang aman dari serangan ini, meski teknik ini memakan waktu yang lama jika dihadapkan pada password yang rumit. Seperti yang diketahui bersama bahwa sebagian besar dalam proses hacking menggunakan sistem operasi linux lebih rincinya yaitu distro kali linux, namun ada juga yang menggunakan proses hacking yaitu password attacker hanya menggunakan windows dengan bantuan tools tertentu seperti hashcat dan lain sebagainya. Dalam hal teknik attack yang dilakukan password attack dapat menggunakan 2 cara yaitu dengan menggunakan wordlist yang akan digunakan oleh tool dan akan dicoba kata demi kata yang ada di dalam wordlist tersebut, cara lainnya adalah menggunakan serangan brute-force yang mana cara ini akan berjalan dengan mencoba semua kemungkinan kunci yang digunakan pada password.

Penulis harus memastikan bahwa tulisannya tidak mengandung unsur plagiasi. Artikel yang sudah terbit sebagai prosiding, tidak diterima untuk terbit di jurnal ini tanpa melalui proses lebih lanjut untuk melengkapi tulisan dan data hasil akhir penelitian.

2. TINJAUAN PUSTAKA

2.1. Tools BarsWF

BarsWF merupakan password attacker yang base on hash MD5 untuk menghitung jumlah hash terbesar dengan secepat mungkin, tools ini dibuat dengan menggabungkan teknologi lama dengan teknologi CUDA yang terbaru mengkombinasikan dengan Processor AMD dan GPU NVIDIA Geforce 8 atau lebih sebagai syarat untuk dapat menjalankannya, tools ini dapat diakses multi OS seperti Windows, Linux maupun MacOS. BarsWF dikembangkan oleh Svarychevaski Michail untuk melakukan proses brute force terhadap single hash md5 dengan bantuan CPU dan GPU. Dengan perbandingan NVIDIA 9600GT/ C2D 3Ghz CUDA dapat men generate sekitar lebih dari 350 juta/detik key, sedangkan dengan versi SSE2 dapat mengakumulasi generate sekitar 108 juta/detik

2.2 HashCat

Hash cat adalah tools pemulihan kata sandi yang memiliki basis kode berpemilik hingga 2015, tetapi kemudian dirilis sebagai perangkat lunak Open Source. Tools ini tersedia untuk beberapa OS, seperti Linux, OS X dan Widows. Contoh algoritma hashing yang didukung hashcat adalah format LM hash , MD4 , MD5 , SHA-family dan Unix Crypt serta algoritma yang digunakan di MySQL dan Cisco PIX. Algoritma-algoritma tersebut dapat dipecahkan dalam waktu yang lebih singkat dengan hashcat berbasis GPU. Hashcat menawarkan jenis mode serangan sebagai berikut: Brute-Force Attack, Combinator Attack, Dictionary Attack, Fingerprint Attack, Hybrid attack, Mask attack, Permutation attack, Rule-based attack, Table-Lookup attack, Toggle-Case attack, dan PRINCE attack.

2.3 Hash Cracker Console

Hash Kracker Console adalah alat baris perintah all-in-one untuk mengetahui kata sandi dari Hash. Saat ini mendukung pemulihan kata sandi dari jenis Hash populer berikut : MD5, SHA1, SHA256, SHA384, SHA512. Pola penyerangan yang digunakan berdasarkan pola -force crack yang membuat tools ini memiliki baris perintah yang membuat tools berjalan lebih cepat dan mudah untuk otomatisasi. Ini adalah alat yang sepenuhnya portabel dan termasuk penginstal juga.

3. METODOLOGI PENELITIAN

Pengambilan metode penelitian yang dilakukan oleh penulis berdasarkan dari penggunaan data dari penelitian sebelumnya, membaca beberapa jurnal lalu dibandingkan dengan cara melakukan pengujian secara berurutan dengan melakukan 5 kali percobaan dalam melakukan password attack. Metode

penelitian saat ini menggunakan 2 kategori serangan yang berbeda yaitu dictionary attack dan brute force. Penelitian ini diawali dengan melakukan studi literatur mengenai pengujian yang dilakukan dengan mencari informasi yang berkaitan dengan penelitian ini, proses dalam penelitian ini dilaksanakan dengan langkah sebagai berikut:

1. Metode Pengumpulan Data

   Metode ini dilakukan dengan membaca beberapa penelitian, artikel, dan buku yang berhubungan dengan penelitian.
2. Melakukan Pengujian

   Pada metode ini dilakukan pengujian pada masing-masing tools sebanyak 5 kali pengujian pada 2 kategori serangan yang berbeda. Hal ini bertujuan untuk mendapatkan data-data yang akan digunakan sebagai dasar dalam perbandigan tools ini. Data-data yang dicari diantaranya adalah:
   - Waktu Serangan
   - Penggunaan CPU
   - Penggunaan Memory
3. Melakukan Perbandingan

   Pada tahap ini dilakukan perbandingan berdasarkan dari hasil data yang didapatkan dari pengukuran yang dilakukan sebelumnya. Sehingga menghasilkan sebuah kesimpulan, yaitu tools apa yang unggul dalam segi waktu dalam melakukan serangan.

   Pada penelitian ini menggunakan laptop dengan sistem operasi Windows dengan spesifikasi laptop seperti berikut: Ram 4 GB, Prosesor i3-600U 2.0GHz, VGA NVIDIA MX110 2 GB, SSD 256 GB. dan juga sebanyak 5 list password yang telah di hashing dengan tipe hash MD5, yaitu:

Tabel 1. Daftar *hash password*

Nomor	***Hash Password***	***Password***
1	768d2bc3aae9b6778f0f298914012db8	undiksha
2	2279dd0e25ab909ee1beaae5b6290bcf	Pastibisa
3	1b37c206a3f3c106057abc80fcf50f45	dDrawX09
4	3420ebfbd8460a5b02d3d99acce13ccd	Bagas@123
5	1d3bfb7710fccec7b5a1dac05c15cb07	N4z1^8

4. HASIL DAN PEMBAHASAN

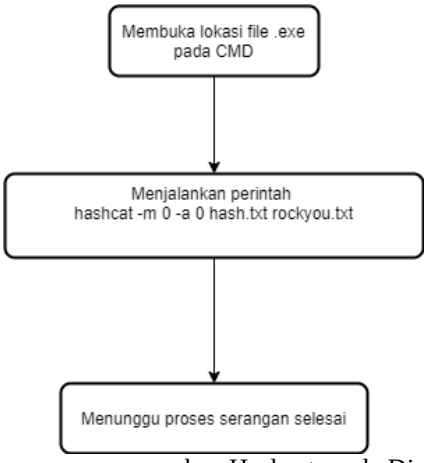
1) Pengujian *Tools* Menggunakan Mode *Dictionary Attack*

a. BarshWF

Pada mode serangan Dictionary Attack tools BarshWF tidak dapat melakukan nya, hal ini dikarenakan tools ini tidak memiliki fitur serangan ini.

b. Hashcat

Pada mode serangan Dictionary Attack tools Hashcat dapat di jalan kan dengan urutan cara sebagai berikut :



Gambar 1. Alur cara menggunakan Hashcat mode Dictionary Attack

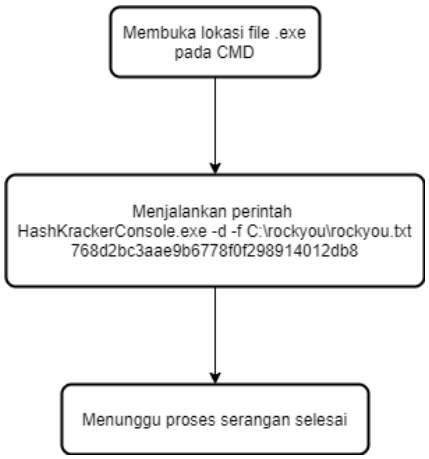
Pada perintah yang dijalankan tersebut dapat dijabarkan sebagai berikut: hashcat -m 0 (*type hash* md5) -a 0 (mode serangan *dictionary attack*) FileHash(.txt) Wordlist(.txt). Untuk wordlist yang digunakan disini telah diatur agar *password* yang ingin di *cracking* dapat di deteksi. Dari 5 kali pengujian yang telah di lakukan didapatkan hasil seperti tabel di bawah:

Tabel 3. Pengujian Hashcat pada *Dictionary Attack*

Nomor Pengujian	Waktu Serangan	Penggunaan CPU	Penggunaan Memory
1	1 detik	5%	70%
2	1 detik	6%	65 %
3	2 detik	5%	68%
4	5 detik	5%	70%
5	5 detik	6%	70%

c. Hash Cracker Console

Pada mode serangan *Dictionary Attack tools* Hash Kracker Console dapat di jalan kan dengan urutan cara sebagai berikut :



Gambar 2. Alur menggunakan Hash Kracker Console pada *Dictionary Attack*

Pada perintah yang dijalankan tersebut dapat dijabarkan sebagai berikut: HashKrackerConsole.exe –d (sebagai jenis serangan *dictionary*) –f (lokasi *dictionary file*) (*password* yang telah di *hash*). Untuk *wordlist* yang digunakan disini telah diatur agar *password* yang ingin di *cracking* dapat di deteksi. Dari 5 kali pengujian yang telah di lakukan didapatkan hasil seperti tabel di bawah

Tabel 4. Pengujian Hash Kracker Console pada *Dictionary Attack*

Nomor Pengujian	Waktu Serangan	Penggunaan CPU	Penggunaan Memory
1	47 ms	5%	5%
2	1 detik	5%	5%
3	2 detik	5%	5%
4	4 detik	5%	5%
5	4 detik	5%	5%

2) Pengujian Tools Menggunakan Mode Brute Force

a. BarsWF

Pada mode serangan Brute Force tools BarshWF dapat di jalan kan dengan urutan cara sebagai berikut :

Gambar 3. Alur cara menggunakan BarsWF mode Brute Force

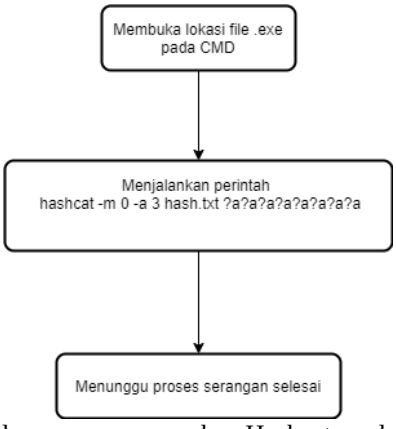
Pada perintah mengubah charset dan hash pada file barswf.cfg memiliki penjabaran sebagai berikut: charset, sebagai setting untuk character yang akan digunakan, charset ini terdiri dari 4 jenis yaitu “a” sebagai lambang character lower case, “A” sebagai lambang character upper case, “0” sebagai lambang angka, dan “~” sebagai lambang simbol. Kemudian hash, sebagai hash password yang telah diketahui. Dari 5 kali pengujian yang telah di lakukan didapatkan hasil seperti tabel di bawah :

Tabel 5. Pengujian BarsWF pada *Brute Force*

Nomor Pengujian	Waktu Serangan	Penggunaan CPU	Penggunaan Memory
1	4 menit	70%	10%
2	10 menit	73%	10%
3	13 menit	73%	10%
4	32 menit	75%	10%
5	34 menit	77%	10%

b. Hashcat

Pada mode serangan Brute Force tools Hashcat dapat di jalan kan dengan urutan cara sebagai berikut:



Gambar 4. Alur cara menggunakan Hashcat mode Brute Force

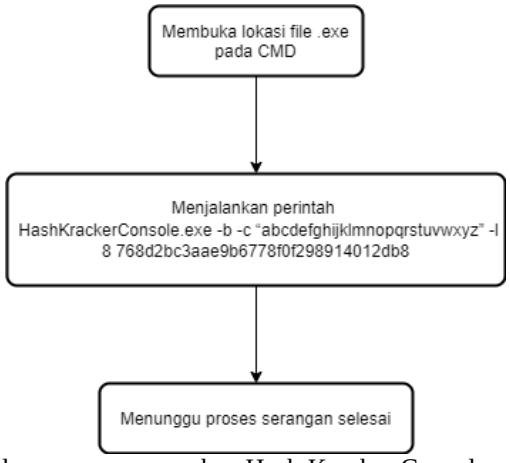
Pada perintah yang dijalankan tersebut dapat dijabarkan sebagai berikut: hashcat -m 0(tipe serangan md5) -a 3 (mode serangan brute force) FileHash ?a (set charset lowercase). Dari 5 kali pengujian yang telah di lakukan didapatkan hasil seperti tabel di bawah:

Tabel 6. Pengujian Hashcat pada *Brute Force*

Nomor Pengujian	**Waktu Serangan**	**Penggunaan CPU**	**Penggunaan Memory**
1	1 detik	5%	70%
2	30 detik	5%	70%
3	1 menit 3 detik	6%	70%
4	8 menit	10%	77%
5	10 menit	13%	80%

c. Hash Cracker Console

Pada mode serangan Brute Force tools Hash Kracker Console dapat di jalan kan dengan urutan cara sebagai berikut :



Gambar 5. Alur cara menggunakan Hash Kracker Console mode Brute Force

Pada perintah yang dijalankan tersebut dapat dijabarkan sebagai berikut: HashKrackerConsole.exe -b(tipe serangan brute force) -c(charset yang akan digunakan) -l(maksimal length password) (password hashes). Dari 5 kali pengujian yang telah di lakukan didapatkan hasil seperti tabel di bawah:

Tabel 5. Pengujian Hash Kracker Console pada *Brute Force*

Nomor Pengujian	Waktu Serangan	Penggunaan CPU	Penggunaan Memory
1	14 jam	24%	10%
2	18 jam	30%	15%
3	30 jam	33%	14%
4	40 jam	40%	26%
5	44 jam	39%	27%

3.1 Hasil

Dari hasil pengujian sebelumnya dapat di rata-rata kan seperti dibawah:

a. ***Perbandingan Mode Serangan Dictionary Attack***

Tabel 6. Tabel Perbandingan rata-rata Mode Serangan Directory Attack

Perbandingan	**Hashcat**	**BarsWF**	**Hash Kracker Console**
Waktu Serangan	2,8 detik	-	2,6 detik
Penggunaan CPU	5%	-	5%
Penggunaan Memory	69%	-	5%

b. ***Perbandingan Mode Serangan Brute Force***

Tabel 7. Tabel Perbandingan rata-rata Mode Serangan Brute Force

Perbandingan	Hashcat	BarsWF	Hash Kracker Console
Waktu Serangan	5 menit	19 menit	29 Jam
Penggunaan CPU	8%	74%	33%
Penggunaan Memory	73%	10%	18%

5. Kesimpulan Dan Saran

Dalam serangan *password attacker* banyak sekali cara yang bisa dilakukan untuk memecahkan *password* atau kode yang ada di sistem, salah satunya dengan teknik serangan *brute force* dan *dictionary attack* yang sangat populer di kalangan dunia *cyber security*. Dengan *tools* yang sangat banyak sekali di internet dengan berbagai ragam cara yang berbeda di setiap toolnya dalam melakukan serangan. Hal tersebut dapat mencoba dari berbagai kemungkinan yang dapat dipecahkan dari beberapa *tools* yang tersedia. *Tools* BarsWF, HashCat, dan Hash Kracker Console merupakan *base on brute force* dan *wordlist* sebagai teknik serangan yang digunakan. Ketiga *tools* tersebut memiliki karakteristik yang hampir sama dengan *mengenerate* hasil dari hash MD5 menjadi *password* STRING pada umumnya. Dengan beberapa metode uji coba yang dijalankan maka dapat memiliki hasil yang sangat berbeda pada setiap *tools* mulai dari waktu serangan, penggunaan CPU yang digunakan untuk *tools* tersebut, serta memakan jumlah *memory* yang diperlukan untuk bisa jalan.

Secara general memang tools Hashcat yang kinerjanya unggul dari kedua tools yang dibandingkan, dengan mode serangan brute force attack, hal tersebut dapat diketahui dari beberapa bandingan seperti rata-rata waktu serangan hanya membutuhkan waktu 5 menit, kondisi, penggunaan CPU 8%, serta penggunaan *memory* 73% yang dialokasikan oleh *tools* Hashcat. Sedangkan dengan mode serangan *Dictionary attack tools* yang dibandingkan lebih unggul adalah Hash Cracker Console dengan rata-rata waktu serangan 2,6 detik, dengan penggunaan CPU 5%, dan memakan *memory* 5%. Memang setiap tools itu berbeda tingkat efektifitas tergantung dari mode serangan yang digunakan dan bergantung juga kembali kepada kebutuhan.

DAFTAR PUSTAKA

[1] Achmady, S. (2017). Analysis Dictionary Attack Dan Modifikasi Password Cracking Serta Strategi Antisipasi. *Jurnal Sains Riset*, *7*(1). https://doi.org/10.47647/JSR.V7I1.12

[2] Sarah Hapsari, N., Fatman, Y., & Penulis Korespondensi, E. (2020). Implementasi Metode One Time Password pada Sistem Pemesanan Online. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *4*(4), 930–939. https://doi.org/10.30865/MIB.V4I4.2195

[3] Bosnjak, L., Sres, J., & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings*, 1161–1166. https://doi.org/10.23919/MIPRO.2018.8400211

[4] Razzaq, A., Aditya, M., Widya, A., Kuncoro Putri, O., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. https://doi.org/10.34010/GPSJOURNAL.V6I1.6698

[5] Ramadhan, M. S., & Ariyani, P. F. (2018). PENINGKATAN KEAMANAN LOGIN WEBSITE DENGAN IMPLEMENTASI ONE TIME PASSWORD MENGGUNAKAN ALGORITMA SHA1 DAN MD5 BERBASIS MOBILE. *SKANIKA*, *1*(2), 689–696. https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/277

[6] Xia, Z., Yi, P., Liu, Y., Jiang, B., Wang, W., & Zhu, T. (2020). GENPass: A Multi-Source Deep Learning Model for Password Guessing. *IEEE Transactions on Multimedia*, *22*(5), 1323–1332. https://doi.org/10.1109/TMM.2019.2940877

[7] Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019). PassGAN: A deep learning approach for password guessing. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11464 LNCS*, 217–237. https://doi.org/10.1007/978-3-030-21568-2_11/COVER